

New Style



Newsletter of the La Crosse PC Users Group

Volume 23 Number 7

July 2003



Productive Web Searches

By: David Donsky, Member

Have you ever done a search on the web and gotten thousands of pages? Have you tried adding multiple words to the search only to get even more pages? There must be a better way, but what is it? How can you do more productive searches and find what you really want?

First you must understand web site designers really do want you to find their pages. Without going into all the technical details web site designers and search engines use key words to help you find the sites you want. Search engines such as www.yahoo.com, www.altavista.com, and many others; are organized much like the index of a book. The key is to learn how to use this index. (Note: other search engines can be found using the search techniques described below)

So you want to do a search, start by deciding what you want to find, this may seem simple, but to do a productive web search you must think of what makes, what you wish to find unique. Think of two or three words to start, the more unique the better for example if you want to find information on writing a book, "writing" would be better than "literature", then do a trial search, entering your word(s) into one of the search engines noted above or your favorite if you have one, and then clicking on the search button. Here's where the plus (+) comes into play, if you enter more than one word in the search box, most search engines will give you all the pages that have either word in them, this is one of the reasons you get so many pages. By using a (+) before the word, for example entering +writing +book instead of writing book you will get only pages that have both word in them, excluding any that just have one of them, this can be very useful in getting to the pages you want to find without looking at a lot of pages that don't apply.

After you have done this trial search evaluate the results, looking at some of the first ten or so, look at the ones that look like they apply to what you want to find. Did you find pages with the information you were looking for? If so great, your search is done, wasn't that easy? Remember at any point in the process you can stop when you get the results you want

However if you found a lot of pages you don't think fit your subject, think about what these irreverent pages have in com-

July Meeting

July 30th, 7:00pm

Lutheran Hospital Overholt Auditorium

"Preparing Tomorrow's Students"

Using Information Technology in the
La Crosse School District

**Presented By Tom Ward, Director of Information
Technology, School District of La Crosse**

1. Why it is important for students to understand technology
2. How our district is adapting to meet this need
3. How we are using technology to enhance learning
4. Where we are headed in the future

mon. This is where the (-) comes in, to get rid of pages that don't apply add a word that these irrelevant page have in common to the search list with a minus (-) in front to it. In our example add -nonfiction this will remove pages about "non-fiction" from your search, now you have only pages about writing fiction. (Note that these techniques are not perfect and it is possible to still find some "non-fiction" page in your list)

Now have you found what you are looking for? If not, redefine the search by starting the search over with new words to help narrow down the results try +mystery +writing and see how this changes the results. Then try using quotation marks, entering +"mystery writing" this will find only those sites with this exact phrase.

This method of trial searches combined with the redefining of the search after evaluating the results is an excellent way to find information on the web. While you may find things you weren't really looking for, think of it as an adventure! The most important part is to have fun and enjoy the trip through cyber space.

Editors Note: I want to thank David for sharing this with us. I would really like to see more entries written by our members. Everyone has a story (horror stories welcome) about their computer experiences. Although I may not continue as editor, I am sure the next editor would appreciate your entries.

La Crosse PC Users Group (LCPC) Treasurer's and Membership Report May - July 2003

*Dick Dahlby, Treasurer and Membership Chairman
ddahlby@cs.com*

July 21, 2003

Income received in May was \$180.00 from nine membership renewals. They were: Kathleen Gallagher, Kevin Blum, Mike Larson, Shane Lambert, Chuck Whalen, Ernesto Brauer, Jean Troyanek, Chuck Hosler, and George Frisch. Income received in June was \$20.00 from one membership renewal, Eldora Hohlfeld. Thank you all for your continued interest and support.

May expenses were: \$30.00 for annual renewal of our ListServ and Website Hosting services, \$14.80 for postage stamps, and \$13.19 for 25 photocopies of the April edition of the LCPC Newsletter. There were no June expenses. The only July expense to date was \$50.00 for our annual renewal to APCUG.

The LCPC checking account balance as of 07/21/2003 is \$1,114.14.

We presently have 51 enrolled members in LCPC.

Members whose annual membership renewal fees (dues) are presently past due are: (February) Larry Nagy.

There were no membership renewals due in June.

Membership renewals due in July are: Darrell Garner, Robert and Mary Pluntz, Peter Schaettle, and Robert and Delaine Stolpa.

Annual dues are \$20 (individual or couple), and checks should be made payable to La Crosse PC Users Group. Dues may be mailed to either of the following addresses, or paid to me at the July 30 meeting.

La Crosse PC Users Group	Dick Dahlby
P.O. Box 2991	501 Olivet St
La Crosse, WI 54601-2991	La Crosse, WI 54603-1318

Reminder to all members:

If you become more than three (3) months delinquent in paying your membership dues, you will be subject to removal from the ListServ, and from LCPC. So please, be prompt with your renewal fees.

Also, if you change your email address, it is very important to inform LCPC of the change, so that the Membership ListServ (membersonly@lcpconline.com) can be changed accordingly. To do so, please send me an email with your new email address and I will make the change to the ListServ. If you haven't received an email from the ListServ within the last two weeks, please let me know that also, so that I can check on it. Thank you.

Did Microsoft Send This?

MS Customer this is the latest version of security update, the "February 2003 Cumulative Patch" update which eliminates all known security vulnerability affecting Internet Explorer, Outlook and Outlook Express as well as five newly discovered vulnerabilities. Install now to protect your computer from these vulnerabilities, the most serious of which could allow an attacker to run executable on your system. This update includes the functionality of all previously released patches. System requirements Win 9x/Me/2000/NT/XP. This update applies to Microsoft Internet Explorer, version 4.01 and later.

Recommendation: Customers should install the patch at the earliest opportunity. How to install Run attached file. Click Yes on displayed dialog box.

How to use: You don't need to do anything after installing this item. Microsoft Product Support Services and Knowledge Base articles can be found on the Microsoft Technical Support web site. For security-related information about Microsoft products, please visit the Microsoft Security Advisor web site, or Contact us. Please do not reply to this message. It was sent from an unmonitored email address and we are unable to respond to any replies. Thank you for using Microsoft products. Best wishes from Microsoft Corporation Internet Security Division

The message is a hoax, and the attachment is a worm/virus that is particularly virulent. It not only replicates itself but starts deleting files on your hard drive.

Let us look at the message and see how we can tell it is a hoax.

1. Microsoft NEVER-NEVER-NEVER sends out messages with patches or attachments, especially unsolicited ones. At the most, Microsoft will refer you to a secure site where the patch can be downloaded. (Did I say NEVER?)
2. This is a rather good copy of the format used by Microsoft, but look at the first line. There is no capital letter to start the sentence. Also there are a number of grammatical errors as well as format errors.
3. The message is not sent through a Microsoft site, but from a *melrto6.wanadoo.fr* (a french site with no Microsoft connection).
4. Microsoft does not have the named division, although it does have units that deal with security, internet or otherwise.

If you receive this or any other similar message, do not immediately install or run the executable file. Check it out. There are numerous sites devoted to security as well as many usenet groups which report on these matters. Your first line of defense is to contact your User Group officers and ask them.

They will know or will have access to resources to verify or debunk the claims.

Remember to practice "Safe Hex."

Watch out for FIZZER

Another Dangerous Computer Worm

By Ira Wilsker

The Fizzer worm, one of hundreds of newly created computer viruses and worms may reach endemic proportions if more of us do not protect our computers from its potentially damaging payload. Fizzer was first detected by the major antivirus and cyberthreat services on May 8. As I type this, one of the major email filtering services, MessageLabs, has reclassified Fizzer to "high-level alert status", as it is currently infecting one of every 312 emails. Other services are showing that as many as 3 percent of all PCs are already infected with Fizzer. Email is not the only source of Fizzer infection, as it can also be transmitted by AOL Instant Messenger (AIM), and across networks from computer to computer. Many of the documented cases of infection came from file sharing networks, predominately the KaZaA service.

One of the reasons why Fizzer is so dangerous is that it has adopted the tactic used by many of its predecessors, such as the Klez, Bugbear, and Yaha viruses and worms, where it immediately disables any antivirus and firewall protection installed on the infected computer. It is also polymorphic, in that the code can mutate, generating different digital signatures possibly capable of sneaking by recently updated antivirus software. Fizzer is also capable of "dropping" varying code on infected computers, causing a variety of problems. Some antivirus publishers have found that some of the malicious code is itself "buggy", and capable of crashing a computer, which although damaging, was not the original intent of the code.

Once a computer is infected, the worm replicates itself by sending out copies of its mutating-self using a variety of resources likely on the computer. It can send copies of itself using its own integral "SMTP" or email engine, without the need to load whatever email software is utilized on the computer. Fizzer can harvest email addresses and other contact information from the Outlook or Outlook Express contacts list, Windows Address Book (WAB), almost any email addresses found on the computer, as well as from IRC, AOL-IM, KaZaA, and other resources. In addition to replicating itself to all of the email addresses found, it also has the capability of updating itself, changing its code and payload, whenever the computer is connected to the net.

If arriving at the targeted computer via email, it will, again similar to its predecessors, arrive with a "spoofed" or forged "From:" address, concealing the real source of the infection. Since the real sender is difficult to identify, those his computer is infecting will not likely inform the owner of the infected computer. The subject line and message are variable, as are the names and file types of the dangerous payload. The payload will likely carry any one of the common executable file extensions such as .exe, .com, .scr, and .pif. The filenames se-

lected by Fizzer are often the names of legitimate files found on the infected computer. The message bearing the payload may also appear as a "FWD:" (forwarded message) from an acquaintance, as the worm may hijack both the "TO:" and "FROM:" addresses from the infected address book; this is yet another example of how human engineering is utilized to trick a victim into opening or activating the payload. Some of the subject lines reported by the antivirus companies also appear to contain religious messages. One possible hint of an infected email is that many of the messages are sent in German, or use German phrases, as well as English.

Once activated, Fizzer checks for files installed on the computer, and if vulnerable, installs multiple copies of itself to the Windows directory, using a variety of filenames. It also installs utilities to monitor and intercept the software running on the computer, and enables "keylogging", where keystrokes typed by the user can be stored, possibly enabling the theft of passwords, account numbers, email addresses, credit card numbers, and other personally sensitive information. Since Fizzer can access the net and file sharing networks, it is capable of sending this information to a large number of destinations. The antivirus publisher McAfee has detected literally hundreds of possible locations that may receive this stolen data. One method used by Fizzer to disseminate the victims' information is to connect online to an IRC or AOL-IM server, remotely join a chat, and post the information; it is not known if these chats are being monitored to capture this information, or to simply provide a means of randomly disclosing what is stolen from the victim. Fizzer can also connect itself to KaZaA and make the information available to unknown individuals by simple download.

Most of the antivirus websites have a free utility available for download, which can detect and kill most versions of Fizzer. Please do not totally depend on the antivirus software already installed on your computer to protect against Fizzer, because since it is polymorphic, and may have deactivated the antivirus software if the infection preceded the appropriate antivirus update, many users have infected computers and are unaware of it, despite the fact that they believe they are protected. I strongly recommend that one of the free online virus scans be run frequently to detect and kill anything that may have slipped by the antivirus software installed on the computer. Many of these free utilities are listed on my website at www.mycomputershow.com.

Free online scans are available at housecall.antivirus.com, www.pandasecurity.com, www.ravantivirus.com, www.bitdefender.com, and www.mcafee.com. If one of these scans finds that Fizzer is installed, it may be necessary to reinstall your antivirus software and firewall after Fizzer is killed. Again this reiterates the absolute need to have antivirus software installed, running, and updated very frequently.

Editor's Note: See, I am not the only one who uses Panda AntiVirus software. If you haven't tried their free online scan, try it now - it really does work!

SPAM – Bane of the Internet

By Ira Wilsker

I hate it; I absolutely hate it. I open my email in the morning and find up to 100 email solicitations offering illegal cable TV descramblers, cheap prescription drugs without a prescription, devices and treatments for “personal enhancement”, university degrees without attending class, voyeuristic opportunities, and the infamous offers of easy riches from the family members of deceased Nigerian dictators. I can typically spend over a half-hour daily deleting this trash. Most of us find the “unsolicited commercial email” a mere nuisance, but to our internet service providers it has become an expensive proposition to process this “spam” email, as it steals internet bandwidth, hard drive space, and processor time, with the costs passed on to us subscribers. What may even be worse is the blatant fraud and criminal solicitations that many of us experience.

According to a report released by the Federal Trade Commission on April 30 (www.ftc.gov/reports/spam/030429spamreport.pdf), much of the spam mail we receive contains false claims as well as other deceptive, and probably illegal, content. To determine the degree of proliferation and deception in spam, the FTC created what appeared to be private websites containing unique email addresses only used on those sites, and posted material in popular newsgroups and chat areas, again using unique email addresses. During the collection phase, over 11,000,000 spam emails were sent by citizens, or received by the “dummy” email addresses created for this purpose. Since many internet users wonder where and how spammers get their email addresses, the FTC found that 86% of the email addresses used on their websites and newsgroups were harvested and resold by spammers. The FTC also tracked the success rate of the “remove me” links commonly given by spammers, and found that 63% of the remove requests were not honored. The FTC also found substantial misrepresentation in the sample emails analyzed, including false “From:” and “Subject:” lines, often clearly intended to trick the recipient into opening the message. Many of those messages (17% of “Adult” spam with false headers) would then display pornographic images without any regard to the age or emotional status of the recipient.

In the analysis of about 1000 spam emails, the FTC found that 20% of the emails were for what the FTC labeled “Investment or Business Opportunities”, including such offers as work-at-home, franchise opportunities, chain letters, and other non-securities offers. “Adult” spam, consisting mostly of pornography and dating services, accounted for 18% of all spam, while “Financial” spam, consisting of credit card offers, mortgage refinancing, cheap insurance, and other related items composed 17% of spam. Close behind were “Products and Services” (16%), “Health” related spam offering dietary supplements, disease prevention, and physical enhancement (mostly sexual in nature) accounted for 10% of all spam. Only 7% of

the spam was for computer or Internet related equipment or services. It should be noted that all of this spam received by the FTC was indeed unsolicited, and not in response to an inquiry made by FTC staffers, even though many of the emails claimed (falsely) to be a reply to an inquiry, or the result of signing up for an “opt-in” service.

The FTC also investigated the accuracy of the email headers, and found that one-third of all spam mail had false “From:” lines in an attempt to disguise the source of the email. Almost half (46%) of the spams with false “From:” lines appeared to be from an acquaintance of the recipient, apparently to trick the recipient into opening the message. Another 13% of these emails appeared to come from an established business relationship, and 14% had blank sources. Some spammers (3%) try to trick the recipient into opening the messages by showing that the message appeared to be from the recipient himself!

The “Subject:” line of spam was only slightly less deceptive; with 22% of spams containing false subject lines, with one-third of those having a stated subject totally unrelated to the content of the message. 42% of these false subject lines alleged to show some existing business or personal relationship with the recipient. Cumulatively, 44% of all spam mail had false “From:” and/or “Subject:” lines. Personally, I do not understand how anyone could transact business, including possibly sending credit card information, to an unknown individual who is lying about his true identity; that is a real setup for fraud and loss.

The body of the message also often contained deceptive information, with 40% of all spam mail containing one or more falsehoods in the content of the message; of those messages touting “Investment or Business Opportunities”, a full 90% contained false information, while 49% of the “Health” spams had falsehoods. 47% of the travel and leisure related spams contained false information. Considering the “From:”, “Subject:” and body of the spam mail, the cumulative number of false emails rises to 66%, with 96% of all “Investment or Business Opportunities” containing misinformation. Again, it amazes me that so many Internet users are gullible and fall for these deceptions. Despite some states requiring commercial email to contain the prefix “ADV” in the subject line, only 2% of all spam complied.

Then there are the chain letters, which often claim to be legal, even to the point of being endorsed by government agencies. According to the FTC, “Nothing is further from the truth.”

It may get worse – spammers are now targeting our cell phones, and most of us pay to receive text messages, shifting the cost of spam almost totally to us, the recipients.

There is no restriction against any non-profit group using this article as long as it is kept in context, with proper credit given to the author. This article is brought to you by the Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organization of which this group is a member.

The Sorry State of Software...

By George Siegel, PIBMUG's Special Correspondent

For the last six months or so, I've become increasingly irritated by the ever growing amount of junk that comes with every new software release. You know what I'm talking about—registrations, cookies, tray icons, background processes, pop-up screens, newsletters, affiliate programs, ad infinitum.

At first, I thought maybe it was just me; heavy workload and all that. Then, a couple of weeks ago, I helped an old friend set up his new PC and I reinstalled all of his 1997-vintage software including PhotoShop, PageMaker, MS-Office and a half dozen other major apps. I finished in record time. No hassles, no online anything, no sales pitches. It felt great.

Then, over the next few days, I had to deal with the following:

A PC that had suddenly slowed to a crawl after the installation of the 164MB printer driver. (Yes, 164MB of "full printing system" on a \$99 inkjet printer.) I replaced it with the 1.12MB file version from the vendor's website and all returned to normal.

A cheesy checkbook program that analyzes your entries in order to make recommendations on how to get out of debt, and apparently is in a position to offer you a bank loan. George Orwell would be proud.

A new computer that had no Internet Explorer and no Internet Connection Wizard. The two choices were to sign up for—and launch—the preloaded AOL or the preloaded DellNet. My cable-connected client didn't want either one. I finally found Internet Explorer as a hidden file and set up the necessary icons but it was a sad waste of 45 minutes. And of course there were the usual viruses, spyware, pop-ups, etc.

In the midst of all this, I realized the cause of my frustration. My role has traditionally been to "add" software and configuration elements to make a computer do that which a client needed. Today's software does too much. (When was the last time you needed to embed a sound file in your Word document?) I now spend my time loading additional software to block or remove features that no one wanted in the first place. This is nonsense and we shouldn't be accepting it.

So here's where you come in. As user group members, you've probably tested more versions of more apps than most users. Make a list of the most recent, stable versions of all the various applications that don't have all the junk features. The minimum requirements are that they be Y2K compatible and run on 32-bit Windows. Once you have the list finished, you can make it clear to your computing buddies that there is simply no reason to ever pay for newer versions of those programs until—or unless—the junk is removed, and any real needed improvements in functionality are needed.

Here's where to start:

MS-Office 97 does everything that most businesses will ever need. No reason to buy anything newer. If your new PC has

Word 2002 bundled with it, remove it and load Office 97. You'll never have to spend another dime for an office suite.

Quicken 2000 (or thereabouts). It's just a checkbook! Whatever version you have, keep it. If your new computer has a newer version bundled with it, delete it and load your existing version. It will run faster and work just fine.

Okay, you get the idea, right? It will give you a great opportunity to tick off software companies while enhancing your user group position as champion of the little guys.

Hey, Protect Yourself, Willya?

You may remember the last time we had a beer, we briefly discussed the general gullibility of new and untrained Internet Users, and our ability, through experience, to quickly see through most of the scams and ploys one finds on the Web.

Recently, I was at the office of a client with about six employees, all of whom recently received e-mail accounts. In no time at all, they were receiving all sorts of spam. I learned that they had all been engaging in various risky activities including sending each other email greeting cards on a regular basis, each trying to outdo the other.

I explained that things such as e-cards are a no-no because they exist primarily to gather names for spammers. I went on to say that no one would spend hundreds of thousands of dollars to put up a sophisticated e-card system unless they had a way to recover their costs. And that even on the web, you can't get something for nothing.

Their response? The sites seemed friendly. Indeed the sites themselves as well as the e-cards have been created with a disarming, warm and fuzzy feel.

Then the client asked me how to make the spam all go away. I had to tell them that it was too late. They had to either live with, and spend time and energy constantly fussing with spam blockers, or change their e-mail addresses.

I find that my admonishments to clients regarding safe practices are either ignored or rebelled against. It's probably that I'm pressed for time and tend to use a very direct approach ("Stop that, you idiot.")

The job of every user group member is to use your demeanor and verbal skills to present the best practices employed by experienced users in a positive, compelling way. Teach them what would be roughly the online equivalent to street smarts. The idea is to not only give users the needed information, but also to convince them that doing things correctly is much "cooler" than being duped by every ploy that comes along.

Hey, I got a virus! Want some golden rules to prevent getting a computer virus?

1. Don't trust any attachment; scan each one.
2. Update your anti-virus signature today.
3. Perform a quick and free Internet scan with www.comandondemand.com

LCPC Board and Officers

Marian Havlik—President 782-7958
HAVLIKME@aol.com

Chuck Walen—Vice-President 787-6678
cw@centurytel.net

Dick Dahlby—Treasurer 781-9356
Ddahlby@cs.com

Secretary — Office Open

Jack Storlie—Programs 788-6355
JStorlie@charter.net

Shane Lambert—Newsletter Editor 784-9696
shane@shanelambert.com



WWW.APCUG.ORG

LCPC is a member of APCUG

New Style is published eleven times a year, monthly January through October with a combined Nov-Dec issue. General meetings are held in the Overholt Auditorium at the Lutheran Hospital on the last Wednesday of January through October with a combined November-December meeting on the second Wednesday in December. A list of our upcoming meeting topics is available at our web site at <http://www.lcpconline.com>. Thank you, Gundersen-Lutheran, for making this wonderful facility available. Meetings begin around 7:00 PM. Everyone is welcome, attend a meeting or two with no obligation to join.

Membership Dues are \$20 and cover an annual period following the month of payment. Membership entitles you to attend meetings, tap into the corporate wisdom, receive special user group discounts from publishers and others, and receive (and contribute to) this newsletter. You may also obtain software provided by publishers for review of the product.

The monthly newsletter is printed the Wednesday before the meeting, please submit advertisements and articles by the 13th of the month to editor@lcpconline.com. Unsigned articles are written by the editor. Other user groups are welcome to reprint with proper credit to the La Crosse PC Users Group and must include our web page address. Please contact the Newsletter Editor for commercial advertising rates. There is no fee for non-commercial advertisements placed by members.

LCPC
P.O. Box 2991
LaCrosse, WI 54602-2991